AFFIDAVIT

I, Taylor Burns, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state the following:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 6033 Major Circle, Augusta, Georgia 30909, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B. As set forth herein, there is probable cause to believe that the PREMISES contains evidence of crime, instrumentalities, and/or fruits thereof, related to violations of Title 18, United States Code, Sections 1030 (Computer Fraud and Abuse) and 1029 (Access Device Fraud).

THE INVESTIGATING AGENT

2. I am an FBI Special Agent assigned to the Atlanta Field Office Cyber Crimes squad. I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7), as a Special Agent of the FBI. As such, I am empowered to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516, including 18 U.S.C. § 1030 (fraud and related activity in connection with computers).

3. I have received extensive training as a Special Agent at the Federal Bureau of Investigation Academy in Quantico, Virginia. I have completed outside training and college courses in computer programming, networking, and information security. Before I was employed by the FBI, I was a desktop support manager with industry experience maintaining and troubleshooting computer systems and network infrastructure. I am presently assigned to investigate computer crimes, including cases involving computer intrusion and internet

fraud. During my career as a Special Agent, I have conducted investigations that involved the use of computers and electronic communication devices that have been utilized in the commission of crimes.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030 (Computer Fraud and Abuse) and 1029 (Access Device Fraud) been committed.

6. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings for the purpose of this affidavit:

a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

b. A Virtual Private Server ("VPS") is a virtual machine provided by an internet service provider. The VPS runs its own operating system and is functionally equivalent to a dedicated server for many services, but it may share the same physical hardware with other VPS clients.

c. An Internet Protocol ("IP") address is a unique numeric address used by computers on the Internet, and looks like a series of four numbers, each in the range 0-255, separated by periods (for example, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. A domain name is an identification label (such as example.com) that allows users to easily locate a website. Domain names resolve back to specific IP addresses, although multiple domain names can resolve back to the same IP address.

d. Bitcoin is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin is often abbreviated using the acronym BTC. Bitcoin is a decentralized digital currency that is popular in the criminal underworld due to its ability to maintain users' anonymity. Bitcoin uses encryption to verify the transfer of funds and operates independently of a central bank. Bitcoin is similar to paper currency in that the exchange of Bitcoin between individuals is not recorded by financial institutions. Bitcoin are not issued by any government, bank, or company, but rather are generated and controlled through computer software operating via a decentralized, peer-to-peer network. While Bitcoin exist primarily as an internet-based form of currency, it is possible to "print out" the necessary information and exchange Bitcoin via physical medium. Bitcoin is just one of many varieties of virtual currency.

i. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password or PIN needed to access the address. Only the holder of an address's private key can authorize any transfers of Bitcoin from that address to other Bitcoin addresses.

ii. To transfer Bitcoin to another address, the payor transmits a transaction announcement, cryptographically signed with the payor's private key, across the peer-to-peer Bitcoin network. The Bitcoin address of the receiving party and the sender's private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any identifying information. As a result, little-to-no personally identifiable information about the payor or payee is transmitted in a Bitcoin transaction itself. Once the payor's transaction announcement is verified, the transaction is added to the blockchain, a decentralized public ledger that records all Bitcoin transactions. The blockchain logs every Bitcoin address that has ever received a Bitcoin and maintains records of every transaction for each Bitcoin address.

iii. Virtual currencies, including Bitcoin, have known legitimate uses. However, given the ease with which Bitcoin can be used to move funds with high levels of anonymity, Bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds.

FACTS IN SUPPORT OF PROBABLE CAUSE

8. The FBI has been investigating a computer intrusion scheme to defraud at least one company in the Northern District of Georgia, and elsewhere. The scheme involved a hacker who compromised the computer network of the company and illegally sold access to the company's server on the dark web. The server also stored data related to the company's clients as well as facilitated remote access to the clients' networks.

INTERVIEW OF CHIMERA INNOVATIONS, LLC

9. Chimera Innovations, LLC., (Chimera) is an Atlanta based information technology (IT) managed service provider (MSP) who provides client services including IT support, mobile application development, website development, and software support.

10. Chimera used Vultr, a Canadian based VPS company, for their cloud server needs, which stored their clients' company data. Chimera's administrative Vultr panel gave them direct access to all their clients' servers as well as other critical company data such as passwords. One Chimera employee (EMPLOYEE A) had an administrator account in the Vultr panel. However, unbeknownst to him, a second admin account had been created. The name of the account was mbritt@chimerainnovations.com and it was created on May 14, 2019. The account belonged to MARQUAVIOUS BRITT (BRITT), who was a former employee of Chimera. At the time the account was created, BRITT was among the personnel who knew the Vultr administrator's password. EMPLOYEE A believed BRITT

logged into EMPLOYEE A's account to create it because a new admin account can only be created by an existing admin account.

11. BRITT was hired by Chimera on May 6, 2019 and was terminated on June 24, 2019. BRITT was a disgruntled employee who was terminated for failure to complete tasks assigned to him. According to EMPLOYEE A, BRITT often expressed his interest in computer hacking to his colleagues.

CYBER ATTACK ON CHIMERA INNOVATIONS, LLC

12. On September 30, 2019, an individual using the online moniker "w0zniak" created a post on a dark web forum which advertised access to a US-based MSP for $600 USD, payable in Bitcoin. w0zniak suggested the access he was offering would enable administrator access to approximately 20 clients hosted on the target system's admin panel. w0zniak's post states as follows:

> i. I'm selling access to a MSP. They're located in the U.S. , eastern side. Their servers are primarily Windows and they're hosting the servers on Vultr which is a VPS [Virtual Private Server]. I have admin access to the hosting panel, passwords for each client is provided and you'll access them through RDP. Their client list is sort of extensive with about 20 in total, notably several law offices, accounting firms, food industry company, and a pharmaceutical company, job staffing company, etc. I'm asking for $600 BTC. If you're interested message me here or on wikr, "w0zniak", i'm also on jabber w0zniak@blabber.im. I can provide photos if requested.

13. On October 10, 2019, the FBI began communicating with w0zniak through a confidential human source (CHS).[1] Through communications with w0zniak, the FBI successfully purchased access to the compromised MSP via Bitcoin. During the communications, w0zniak provided a Bitcoin address beginning with 3PsSX, which was to be used for payment. Additionally, w0zniak provided credentials to the MSP's administrator panel, which listed the username "mbritt@chimerainnovations.com" and password "Quay#7816!". Based on the domain listed as part of the username, the FBI determined that the compromised administrator account belonged to Chimera, which was confirmed by EMPLOYEE A. Furthermore, database research revealed that "7816" is the last four digits of BRITT's social security number.

COINBASE

14. Through analysis of the Bitcoin blockchain, the FBI identified that the Bitcoin address 3PsSX, which was provided by w0zniak, was held at Coinbase[2]. In response to legal process, Coinbase provided records related to the owner of the Bitcoin address beginning with 3PsSX. Coinbase records identified the owner of the Bitcoin address as BRITT. Coinbase records included a copy of BRITT's driver's license and listed a Chase Bank account ending in 4417. In addition, Coinbase listed a PayPal account for BRITT using the email address xthanos@protonmail.com. The information provided in Coinbase records

[1] The CHS has provided reliable and corroborated information to the government for over two years. CHS reporting has continually been timely, detailed, and accurate. CHS has provided information on multiple occasions that has resulted in open investigations and identified subjects. CHS has also successfully identified multiple victims which were positively confirmed during victim notifications. CHS has no criminal history and no known Giglio issues.

[2] Coinbase is a California-based digital currency wallet and platform where consumers can transact digital currencies like bitcoin, Ethereum, and Litecoin.

such as BRITT's driver's license, social security number, phone number, birthdate, and email address match BRITT's Chimera employment documentation.

15. A review of transaction records and login history for the Coinbase account identified that on October 10, 2019, IP address 75.76.203.92 was used to access the account. Additionally, this IP address was used to login to the account around the same time that the account was credited in the amount of which w0zniak sold access to Chimera's administrator panel, which was approximately $440. Later that day, approximately $440 was transferred from BRITT's Coinbase account to his PayPal account. During this transaction, BRITT utilized the IP address 75.76.203.92.

PAYPAL

16. In response to legal process, PayPal provided the FBI records for an account belonging to BRITT. PayPal records identified that on October 10, 2019, BRITT's PayPal account received approximately $441.00 USD from Coinbase. That same day, funds were transferred from BRITT's PayPal account to BRITT's Chase account ending in 4417. Furthermore, IP address 75.76.203.92 was used to login to BRITT's PayPal account on October 10, 2019.

JPMORGAN CHASE

17. In response to legal process, JPMORGAN CHASE (CHASE) provided account records for BRITT's bank account. Analysis of BRITT's bank account showed the aforementioned PayPal transfer. BRITT's bank account also showed at least one deposit into his account from Chimera during the timeframe of his employment. In addition, BRITT's

bank account showed at least one transfer to an individual named [D.B.]. Additionally, the Chase account number matches the financial account linked to BRITT'S Coinbase account.

IP ADDRESS LINK TO PREMISES

18. Through open source research, the FBI determined IP address 75.76.203.92 resolved to Wide Open West, who is an Internet Service Provider (ISP). In response to legal process, Wide Open West provided subscriber information for the IP address 75.76.203.92. Wide Open West records showed IP address 75.76.203.92 was registered to D.B. and listed the subscriber address as 6033 Major Circle, Augusta, GA 30909 (PREMISES). The FBI later determined D.B. and BRITT are in a relationship.

19. On January 14, 2020, the FBI spoke with an employee of Victim-2 (BRITT'S current employer). The employee advised the FBI that BRITT'S listed residence on employee documents was 6033 Major Circle, Augusta, GA 30909 ("PREMISES"). BRITT'S emergency contact was D.B., which listed D.B. as his domestic partner.

SOCIAL MEDIA

20. Open source research conducted by the FBI revealed a Twitter account associated with BRITT. In response to legal process, Twitter provided subscriber information and IP login history for BRITT'S account. Twitter records showed IP address 75.76.203.92 was utilized to login to the account approximately 50 times between October 18, 2019 and November 25, 2019.

VULTR ACCESS LOGS

21. According to Chimera, Chimera's Vultr access logs show that on October 12, 2019, IP address 75.76.203.92 was used to login to Chimera's Vultr administrator account. The aforementioned login occurred after BRITT'S employment was terminated.

22. Based on my training and experience and the above information, there is probable cause to believe that BRITT made unauthorized access to CHIMERA from the PREMISES after he no longer worked for the company.

23. Furthermore, based on the logins to CHIMERA'S Vultr account from the PREMISES around the time frame of the dark web w0zniak sale, there is probable cause to believe that evidence related to the dark web sale, and violations of Title 18 U.S.C. Sections 1029 and 1030 will be found at the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

24. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Also based on my knowledge, training, and experience, I am aware that connections were made to Chimera's administrator panel from computer(s) located at the PREMISES. Based on the IP records obtained, there is reason to believe that there is a computer system currently located on the PREMISES.

26. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to access another computer network without authorization over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

27. Searching storage media for the evidence described in the attachments may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging

is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the

entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

29. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

30. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint- recognition features are increasingly common on modern digital devices.

31. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

32. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial¬ recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy SB (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

33. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly,

retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy SB and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

34. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

35. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has

not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button.

36. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

37. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to MARQUAVIOUS BRITT who is reasonably believed by law enforcement to be a user of a biometric sensor-enabled device that is (a) located at the PREMISES and (b) falls within the scope of the warrant: (1) compel the use of the person's thumb- and/or fingerprints on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

38. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

CONCLUSION

39. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.